FAULT INTOLERANT CIPHER CHAINING

ABSTRACT OF THE DISCLOSURE

A method and system for producing, e.g., tamper-resistant software such that the software is fault intolerant, thereby complicating hacking attacks, includes undertaking several iterations of forward plain text chaining and backward plain text chaining through the blocks. Essentially, during forward chaining a block is scrambled using a single round of an appropriate algorithm such as DES, and then it is XORed with the plain text of the next block. The result of the XOR is then scrambled, and then XORed with the plain text of the next block, and so on. At the end of the stream, the process is repeated in reverse, from last block to first. The cycles are repeated for the desired number of rounds, e.g., 16.

Doc No. 2000-0063